

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-075601

(43)Date of publication of application : 26.03.1993

(51)Int.Cl.

H04L 9/22

(21)Application number : 03-235007

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 13.09.1991

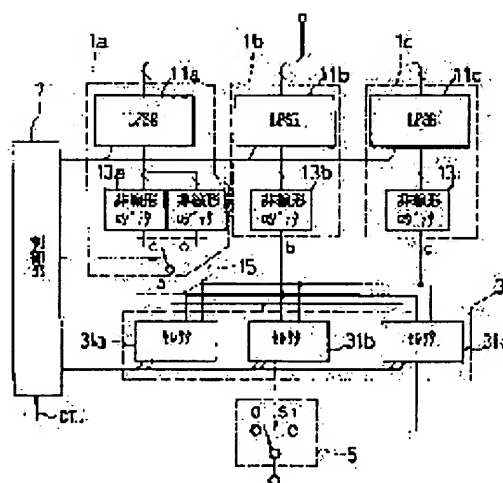
(72)Inventor : KITAGAWA KAZUO

(54) PSEUDO RANDOM NOISE GENERATOR

(57)Abstract:

PURPOSE: To provide a secure PN generating circuit from which the structure of a PN signal and of the PN generating circuit are not analyzed.

CONSTITUTION: The PN generating circuit is provided with noise generating means 1a, 1b, 1c, a replacement section 3 and a control section 7. The noise generating means 1 is constituted of a linear feedback shift register means 11 outputting plural pseudo random noise sequences with a control signal selecting plural sequences and a nonlinear logic 13 fetching plural output signals from the register means 11 and outputting one noise signal. The noise signal from each of the noise generating means 1a, 1b, 1c is given to the replacement section 3, in which various combinations are selected by using a switching signal S_k from the control section 7. The setting of the revision, switching and replacement of the noise generating means 1a, 1b, 1c and the replacement section 3 is revised at any time via the control section 7 and the analysis of the structure of a PN signal and a PN generating circuit is disable.



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平5-75601

(43)公開日 平成5年(1993)3月26日

(51)Int.Cl.⁵

H 0 4 L 9/22

識別記号

庁内整理番号

F I

技術表示箇所

7117-5K

H 0 4 L 9/ 04

審査請求 未請求 請求項の数3(全 7 頁)

(21)出願番号 特願平3-235007

(22)出願日 平成3年(1991)9月13日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 北川 和雄

神奈川県横浜市磯子区新杉田町8番地 株

式会社東芝映像メディア技術研究所内

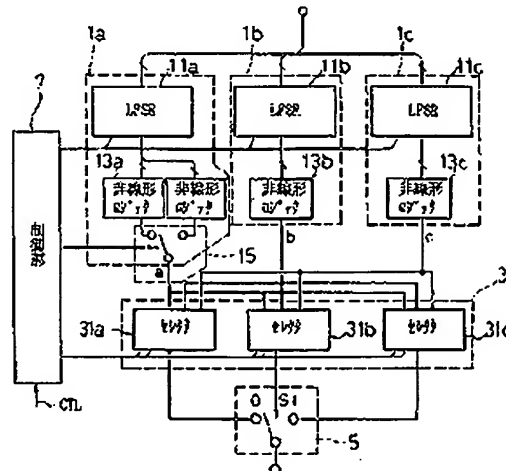
(74)代理人 弁理士 三好 秀和 (外4名)

(54)【発明の名称】 疑似ランダムノイズ発生装置

(57)【要約】

【目的】 PN信号及びPN発生回路の構成を分析されない安全なPN発生回路を提供すること。

【構成】 PN発生回路は、ノイズ発生手段1a、1b、1cと、入替え部3と、制御部7とを備えている。ノイズ発生手段1は、複数のシーケンスを選択する制御信号により複数の疑似ランダムノイズシーケンスを出力する線形フィードバックシフトレジスタ手段11と、前記レジスタ手段11からの複数本の出力信号を取り込み、1本のノイズ信号を出力する非線形ロジック13で構成されている。各ノイズ発生手段1a、1b、1cからのノイズ信号は、入替え部3により制御部7からの切替信号Skにより各程の組合せに入れ換える。ノイズ発生手段1a、1b、1c、入替え部3の変更、切替え、入れ換えの設定を制御部7を介して随時変更可能とし、PN信号、PN発生回路の構成の分析不可能とした。



【特許請求の範囲】

【請求項1】 入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と、

入力される制御信号によって出力を変更し得る非線形ロジックで構成され前記線形フィードバックシフトレジスタ手段に接続される非線形ロジック手段と、

外部から入力される信号によって線形フィードバックシフトレジスタ手段と非線形ロジック手段に制御信号を与える制御手段とを有することを特徴とする疑似ランダムノイズ発生装置。

【請求項2】 入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と、

この線形フィードバックシフトレジスタ手段に接続され、入力される制御信号によって当該複数の線形フィードバックシフトレジスタ手段からの信号を入れ換える入換え手段と、

外部から入力される信号によって線形フィードバックシフトレジスタ手段と入換え手段に制御信号を与える制御手段とを有することを特徴とする疑似ランダムノイズ発生装置。

【請求項3】 入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と、

入力される制御信号によって出力を変更し得る非線形ロジックで構成され前記線形フィードバックシフトレジスタ手段に接続される非線形ロジック手段と、この非線形ロジック手段に接続され、入力される制御信号によって当該複数の非線形ロジック手段からの信号を入れ換える入換え手段と、

外部から入力される信号によって線形フィードバックシフトレジスタ手段と非線形ロジック手段及び入換え手段に制御信号を与える制御手段とを有することを特徴とする疑似ランダムノイズ発生装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、デジタルデータや音声のデータ列にスクランブルをかけるために使用される疑似ランダムノイズを発生する疑似ランダムノイズ発生装置に関する。

【0002】

【従来の技術】 従来、疑似ランダムノイズ発生装置は、デジタルデータ列や音声のデータ列にスクランブルをかけるために使用される疑似ランダムノイズ（以下、単にPNと略称する）を発生するものとして提供されている。具体的には、例えば衛星放送の有料化の実現のために、このPN発生回路が使用されている。すなわち、衛星放送では音声やPCMデジタルデータで伝送しているが、これを有料化する場合には、一般的に音声のPCM

デジタルデータとPN系列とを排他的論理和（EXOR）回路で排他的論理和をとることによりスクランブルをかけ、盗聴を防止するようにしている。

【0003】 図4は、上述したPN発生回路の簡単な構成例を示すブロック図である。図4に示すPN発生回路は、リニアフィードバックシフトレジスタ（LFSR：linear feedback shift register）で構成した例であり、シフトレジスタ401、403、405、407と、EXOR回路109とを備え、シフトレジスタ401をX、シフトレジスタ403をX'、シフトレジスタ405をX''、かつシフトレジスタ407をX'''とすると、その出力が(X' + X + 1)となるようにしている。

【0004】 そして、上記PN発生回路の出力は次のようになる。すなわち、例えば全“1”を読み込み、LFSRを動作させた場合、各レジスタ401、403、405、407の内容は、表1に示すようになる。

【0005】

【表1】

	X	X'	X''	X'''
1	1	1	1	1
2	1	0	1	1
3	1	0	0	1
4	1	0	0	0
5	0	1	0	0
6	0	0	1	0
7	0	0	0	1
8	1	1	0	0
9	0	1	1	0
10	0	0	1	1
11	1	1	0	1
12	1	0	1	0
13	0	1	0	1
14	1	1	1	0
15	0	1	1	1
16	1	1	1	1

【0006】 上記表1の16番目のクロックは、元の全“1”の状態に戻って以下これをくり返すことになる。このとき、レジスタ407の出力(X''')は“111000100110101”の反復となる。このようなPN発生回路は、たとえレジスタの段数をn段に増加させて周期を長くしても、高々(2^n - 1)にしかならず、極めて簡単にPN系列がサーチされてしまう虞が生じる。

【0007】 この点を解消するために、図5に示すPN発生回路が提案されている。この図5に示すPN発生回

路は、LFSR511, 513, 515を有しており、各LFSR511, 513, 515には、32〔ビット〕のスクランブル鍵である初期値IKの13〔ビット〕、11〔ビット〕、8〔ビット〕として入力される。各LFSR511, 513, 515には、ロードタイミングLT、シフトクロックSCkが入力されている。各LFSR511, 513, 515には非線形ロジック(NF)517, 519, 521がそれぞれ接続されており、各NF517, 519, 521は各6〔ビット〕の入力を一本の出力にする。NF519は、切

【0008】このように非線形化されて周期が長くしたPN発生回路を使用し、さらにこれをカスタムIC化することにより、實際上PN信号の構成がサーチされないようにしている(「電気通信技術審議会答申、諮問第17号、昭和63年11月28日」)。このようPN発生回路によれば、出力系列を分析してPN信号の構成をサーチする方法で使用するPN信号の構成を分析しても分析が極めて困難であり、極めて安全性が高いといえる。しかしながら、カスタムICチップの内部構成を顕微鏡で覗かれることまで考えると必ずしも安全とはいえない

【0009】

【発明が解決しようとする課題】このように従来のPN発生回路によれば、いくら複雑なPN信号の構成にしても、そのPN発生回路をIC化した後のICのチップを分析される方法に対しては安全といえないという欠点がある。

【0010】そこで、本発明の目的は、この欠点を解消し、PN信号及びPN発生回路そのものの構成を分析されない安全なPN発生回路を提供することにある。

【0011】

【課題を解決するための手段】上記目的を達成するために、本願第1の発明の疑似ランダムノイズ発生装置は、入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と、入力される制御信号によって出力を変更し得る非線形ロジックで構成され前記線形フィードバックシフトレジスタ手段に接続される非線形ロジック手段と、外部から入力される信号によって線形フィードバックシフトレジスタ手段と非線形ロジック手段に制御信号を与える制御手段とを有することを要旨とする。

【0012】本願第2の発明の疑似ランダムノイズ発生装置は、入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と、この

線形フィードバックシフトレジスタ手段に接続され、入力される制御信号によって当該複数の線形フィードバックシフトレジスタ手段からの信号を入れ換える入換え手段と、外部から入力される信号によって線形フィードバックシフトレジスタ手段と入換え手段に制御信号を与える制御手段とを有することを要旨とする。

【0013】本願第3の発明の疑似ランダムノイズ発生装置は、入力される制御信号によって出力を変更し得る複数の線形フィードバックシフトレジスタ手段と、入力される制御信号によって出力を変更し得る非線形ロジックで構成され前記線形フィードバックシフトレジスタ手段に接続される非線形ロジック手段と、この非線形ロジック手段に接続され、入力される制御信号によって当該複数の非線形ロジック手段からの信号を入れ換える入換え手段と、外部から入力される信号によって線形フィードバックシフトレジスタ手段と非線形ロジック手段及び入換え手段に制御信号を与える制御手段とを有することを要旨とする。

【0014】

【作用】上述した構成によれば、複数の線形フィードバックシフトレジスタ手段と非線形ロジック手段の構成を制御信号によって変更すると共に、さらにこれら出力信号を入れ換えの設定を随時変更することを可能にしたことにより、例えICのチップを顕微鏡で分析されたとしてもなお、PN信号及びPN発生回路の構成を分析不可能として安全性を高めたものである。

【0015】

【実施例】以下、本発明について図示の実施例に基づいて説明する。

【0016】図1は、本発明に係る疑似ランダムノイズ発生装置としてのPN発生回路の実施例を示すブロック図である。図1に示すPN発生回路は、3種類のノイズ発生手段1a, 1b, 1cと、これら手段1a, 1b, 1cからの出力信号を入れ換える入替え部3と、入替え部3からの出力を切り換えるスイッチ5と、前記手段1a, 1b, 1cの発生シーケンス及び入替え部3の切り換え制御する制御部7とを備えている。

【0017】ノイズ発生手段1aは、制御部7からの制御信号Scにより複数の疑似ランダムノイズシーケンスを出力する線形フィードバックシフトレジスタ手段11aと、前記レジスタ手段11aからの複数の出力信号を取り込み、1本のノイズ信号を出力する二つの非線形ロジック13ax, 13ayと、非線形ロジック13ax, 13ayの出力の内の一つを制御部7からの切換信号Skで選択するスイッチ15とから構成されている。ノイズ発生手段1bは、複数のシーケンスを選択する制御信号により複数の疑似ランダムノイズシーケンスを出力する線形フィードバックシフトレジスタ手段11bと、前記線形フィードバックシフトレジスタ手段11bからの複数の出力信号を取り込み、1本のノイズ信号を出力する

非線形ロジック13bとから構成されている。ノイズ発生手段1cは、複数のシーケンスを選択する制御信号により複数の疑似ランダムノイズシーケンスを出力する線形フィードバックシフトレジスタ手段11cと、前記線形フィードバックシフトレジスタ手段11cからの複数本の出力信号を取り込み、1本のノイズ信号を出力する非線形ロジック13cとから構成されている。入替部3は、前記各ノイズ発生手段1a、1b、1cからのノイズ信号を、制御部7からの入替信号Seにより各組の組合せに入れ換えるものであり、セレクト31a、31b、31cから構成されている。各セレクト31a、31b、31cは、各ノイズ発生手段1a、1b、1cからの出力信号を取り込み、入替信号Seにより一つ選択する。各セレクト31a、31b、31cの出力はスイッチ5により一つ選択する。スイッチ5は、表2に示す信号が入力されている。

【0018】

【表2】

a	b	c
0	1	S
0	S	1
1	0	S
S	0	1
1	S	0
S	1	0

【0019】なお、上記制御部7は単なるラッチで実現できる。そして、制御部7から出力される制御信号Scは各レジスタ手段11a、11b、11cに各一本入力され合計3本となる。また、切換信号Skは1本、入替信号Seが6種の組合せとすると、この構成は $2^3 \times 2^1 \times 6 = 96$ 種をとりうることになる。この制御部7の制御信号Sc、切換信号Sk、入替信号Seの組合せは*

下位 上位	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	0	1	0	0	1	1	0	0	1	0	0	1	0	1	0
1	1	0	0	1	1	0	0	1	0	0	1	1	0	1	0	1
2	0	1	1	1	0	0	1	0	1	1	0	1	0	1	1	0
3	0	1	0	0	1	1	0	1	0	0	1	1	1	0	0	1

【0023】このように構成された実施例の作用を説明する。

【0024】制御部7は、各レジスタ手段11a、11b、11cに制御信号Scを与える。また、各レジスタ

*随時、送信局側からのコントロール信号CTLで変更することもできるし、このICを組み込んだ受信機に、何らかのキー操作で構成したコントロール信号CTLで組合せを変えられることができるようにする。

【0020】図2は、線形フィードバックシフトレジスタ手段の構成例を示すブロック図である。図2において、線形フィードバックシフトレジスタ手段11a、11b、11cの各構成は基本的に同一であるため、符号a、b、cを取って説明する。線形フィードバックシフトレジスタ手段11は、シフトレジスタ111、113、115、117と、EXOR回路119、121と、アンド回路123、125とからなり、アンド回路123、125に入力される制御信号Scが“1”のときに $(X' + X' + 1)$ の出力が、制御信号Scが“0”のときに $(X' + X + 1)$ の出力が得られるようにしてある。一般にM段のレジスタ手段11a、11b、11cには、周期が $(2^M - 1)$ になるいくつかの構成が知られており、3種以上のときは、制御信号Scを複数本とする必要がある。一般に、“1”と“0”の数を50%づつにし、入力変化に対し相関の少ない出力が出るようにされている。

【0021】図3は、非線形ロジックの構成例を示すブロック図である。非線形ロジック13ax、13ay、非線形ロジック13b、非線形ロジック13cは、一般にアンド回路、オア回路、EXOR回路の組合せで構成できるが、リードオンリメモリ（ROM）を使うのが最も簡単である。図3において、入力端子にスイッチ131を設けて7本のアドレス入力を可能にしている。スイッチ131を通して得た6本のアドレス入力をROM133に取り込み、一本の出力を得ている。ROM133は、表3に示すデータ例が記憶されている。ROM133は、表1に示す上位アドレスを2（ビット）、下位のアドレス4（ビット）に応じた値を出力できる。

【0022】

【表3】

手段11a、11b、11cは、当該制御信号Scにより、例えば図2の構成から分かるように、制御信号Scが“1”なら $(X' + X' + 1)$ の出力が、制御信号Scが“0”なら $(X' + X + 1)$ が得られる。すなわ

ち、制御信号Scが“0”のときは、アンド回路125の出力がフィードバック信号127によらず“0”となり、EXOR回路121の片側の入力が“0”となる。すなわち、EXOR回路121は単なるバッファとなる。また、制御信号Scが“1”のときは、アンド回路123の出力、EXOR回路119の片側の入力が“0”となり、このEXOR回路119が単なるバッファになる。このときは、別のPNシーケンスを発生することになる。このような出力信号を出力するレジスタ手段11aからは複数本の出力が非線形ロジック13ax、13ayに、レジスタ手段11bからは複数本の出力が非線形ロジック13bに、レジスタ手段11cからは複数本の出力が非線形ロジック13cにそれぞれ入力される。非線形ロジック13ax、13ay、非線形ロジック13b、非線形ロジック13cは、それぞれ1本の出力を出す。非線形ロジック13ax、13ayは、制御部7からの切換信号Skにより切り替わるスイッチ15により一つが選択され、ノイズ信号aとして出力する。非線形ロジック13bからのノイズ信号bが、線形ロジック13cからはノイズ信号cがそれぞれ出力される。各ノイズ信号a、b、cは、入替え部3の三つのセレクト31a、31b、31cにそれぞれ入力される。入替え部3のセレクト31a、31b、31cには制御部7から入替信号Seが与えられており、これによりノイズ信号a、b、cの内の一つが選択されて、表2に示すような6種の状態に入替えられる。各セレクト31a、31b、31cの出力は、スイッチ5の“0”、“1”、“S”の入力に供給される。すなわち、三つのセレクト31a、31b、31cは、三本のノイズ発生手段1a、1b、1cからのノイズ信号a、b、cをスイッチ5に

【0025】このように本実施例では、制御信号Sc、切換信号Sk、入替信号Seの組合せは、随時送信局側からのコントロール信号CTLで変更することもできる。このICを組み込んだ受信機に何らかのキイ操作で構成したコントロール信号CTLで組合せを変えられることができるようにしていることから、IC化した内容を分析してもPN発生回路の構成を簡単に変更することが可能であるため、PN発生回路の構成をサーチすることがほとんど不可能である。

*40

*【0026】なお、上記実施例において、3種の方法で説明したが、2種の切替えとすることももちろん可能である。

【0027】また、本実施例によれば、ICをコピーされ海賊版が出回っても簡単にPN発生回路の構成を変更できるため、スクランブル放送への数億円の投資が全く無駄になってしまうことを防止できるという多大な効果を有する。

【0028】

【発明の効果】以上説明したように本発明によれば、わずかな回路の追加により、容易にPN発生回路そのものの構成を変更できるので、たとえICを分析されても十分安全な、PN発生回路を提供することができる。

【図面の簡単な説明】

【図1】本発明の実施例を示すブロック図である。

【図2】本発明で使用するレジスタ手段の構成例を示すブロック図である。

【図3】本発明で使用する非線形ロジックの構成例を示すブロック図である。

【図4】従来のPN発生回路を示すブロック図である。

【図5】従来の他のPN発生回路を示すブロック図である。

【符号の説明】

1a ノイズ発生手段

1b ノイズ発生手段

1c ノイズ発生手段

3 入替え部

5 スイッチ

7 制御部

11a レジスタ手段

11b レジスタ手段

11c レジスタ手段

13ax 非線形ロジック

13ay 非線形ロジック

13b 非線形ロジック

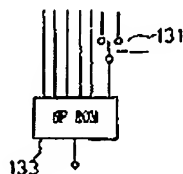
13c 非線形ロジック

31a セレクト

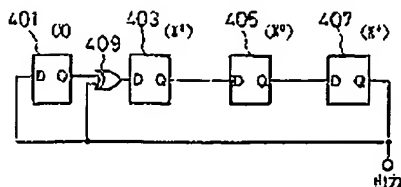
31b セレクト

31c セレクト

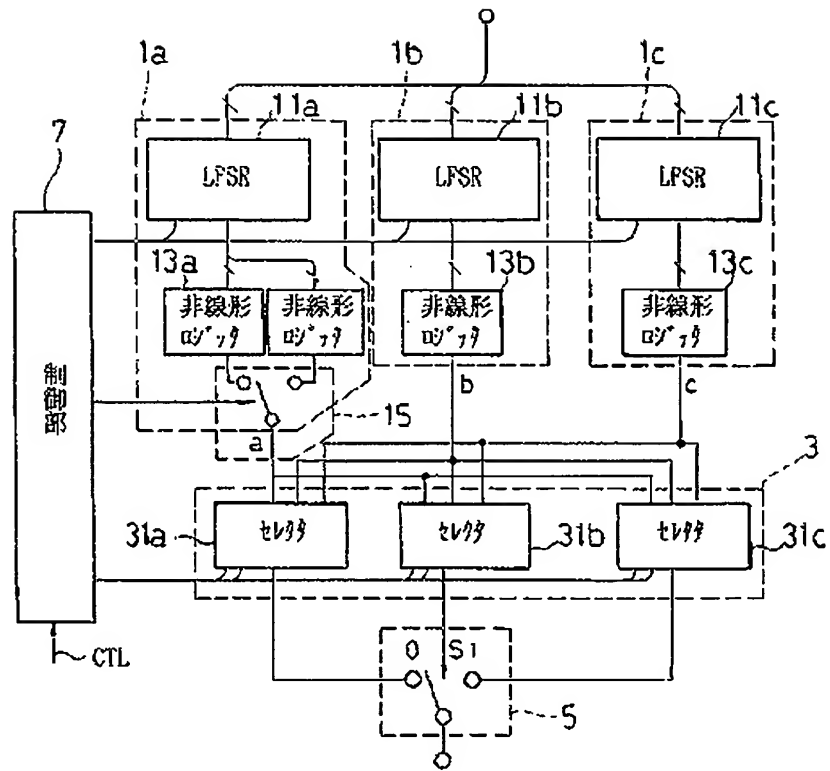
【図3】



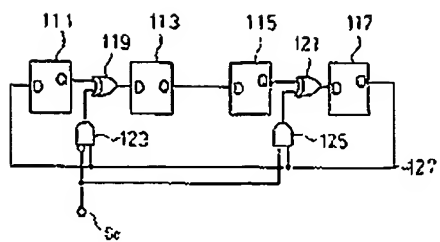
【図4】



【図1】



【図2】



〔図5〕

